رضوانی، شهلا (۱۳۹۷). طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی. *پژوهشنامه کتابداری و اطلاع‌رسانی*، ۸ (۱)، ۳۳۷- ۳۵۶.

دانشگاه فردوسی مشهد
دانشکده علوم تربیتی و روان شناسی

# طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی

شهلا رضوانی[۱]

تاریخ دریافت: ۱۳۹۵/۱۰/۱۱     تاریخ پذیرش: ۱۳۹۶/۰۹/۰۸     DOI: 10.22067/riis.v0i0.61486

**چکیده**

**مقدمه:** مزایای ذخیره‌سازی اطلاعات به‌صورت الکترونیکی سازمان‌ها را در معرض انواع تهدید مانند دست‌کاری اطلاعات مرجع یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی قرار داده است. مطالعۀ حاضر باهدف ارائۀ الگوی استراتژیک مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی انجام شد.

**روش‌شناسی:** در مطالعه‌ای توصیفی‌همبستگی، ۱۹۶ کارشناس و کتابدار کتابخانه‌های دیجیتالی دانشگاه‌های شهر تهران به‌روش هدفمند انتخاب شدند و پرسش‌نامه‌های تحقیق را تکمیل نمودند. روایی و پایایی این پرسش‌نامه‌ها با استفاده از تحلیل عاملی تأییدی و محاسبۀ آلفای کرونباخ تأیید شدند. اطلاعات با استفاده از آزمون‌های توصیفی (میانگین و انحراف استاندارد) و تحلیلی (تحلیل مسیر) بررسی شد.

**یافته‌ها:** اثر متغیرهای خط‌مشی امنیت اطلاعات، معماری اطلاعات، سازمان‌دهی امنیت اطلاعات، توسعۀ سیستم‌های اطلاعاتی، امنیت منابع انسانی و حفاظت محتوا بر امنیت اطلاعات در کتابخانه‌های دیجیتالی در سطح ($P<۰/۰۱$) مثبت و معنادار بود. همچنین در میان متغیرهای موجود در الگو، توسعۀ سیستم‌های اطلاعاتی بیشترین اثر مستقیم را بر امنیت اطلاعات کتابخانه‌های دیجیتالی (۰/۴۴) دارد.

**نتیجه‌گیری:** یافته‌های تحقیق نشان از تأثیر متغیرهای مدل بر امنیت اطلاعات در کتابخانه‌های دیجیتالی دارد. با استفاده از نتایج این پژوهش، برنامه‌ریزان و مدیران کتابخانه‌های دیجیتالی می‌توانند موجبات ارتقای سیستم امنیت اطلاعات کتابخانه‌های دیجیتالی را فراهم آورند.

**کلیدواژه‌ها:** امنیت اطلاعات، مدیریت اطلاعات، کتابخانه‌های دیجیتالی، ارائۀ الگو

۱. مربی، گروه علم اطلاعات و دانش شناسی، دانشگاه پیام نور، تهران، ایران (نویسنده مسئول)، rezvani.shahla@gmail.com

**مقدمه**

حرکت سریع کشورها به‌سوی جامعهٔ اطلاعاتی موجب رشد وسیع سیستم‌ها و سرویس‌های اطلاعاتی و به‌وجودآمدن نوع جدیدی از سازمان با عنوان سازمان‌های مجازی شده است که سازمان‌هایی مبتنی براطلاعات هستند. باتوجه‌به نقش اطلاعات به‌عنوان کالای با ارزش در این سازمان‌ها وجود خطرات و تهدیدات امنیتی [1] که در محیط مجازی و به‌واسطهٔ اتصال به اینترنت به‌وجود می‌آیند. لزوم حفاظت از این اطلاعات ضروری به‌نظر می‌رسد برای دستیابی به این هدف هرسازمان بسته به سطح اطلاعات خود نیازمند طراحی سیستم مدیریت امنیت اطلاعات می باشد تا ازاین طریق بتواند تهدیداتی که سازمان درمعرض آن قرار دارد را شناسایی و مدیریت کند سرمایه‌های اطلاعاتی خود را در برابر این تجاوزات حفاظت نماید و امنیت اطلاعات سازمان را به‌طور پیوسته بهبود بخشد. باتوجه‌به اهمیت نقش اطلاعات جاری در هر سازمان به‌کارگیری سیستم مدیریت امنیت اطلاعات جهت راه اندازی اجرا کنترل چک کردن نگهداری و بهبود امنیت اطلاعات امری حیاتی به‌نظر می‌رسد از این رو سازمان‌ها و شرکت‌ها ناگزیر به دنبال پیاده سازی امنیت هستند که این سیستم باید برمبنای نیازهای سازمان و اهمیت اطلاعات طراحی شود و می‌تواند یک پشتیبان جهت فراهم‌کردن سرمایه‌های اطلاعاتی باشد (Soomro, 2016).

با ورود این فناوری‌ها به کتابخانه‌ها، توجه‌به داده‌ها و اطلاعات موجود در کتابخانه و ارائه آن‌ها به مراجعه کنندگان بیش از پیش مورد توجه قرار گرفته است و کتابخانه‌ها به‌عنوان سازمانی برای ذخیره و بازیابی اطلاعات مورد نیاز کاربران در برآوردن نیاز اطلاعاتی آن‌ها نقش مهمی را ایفا می‌کنند. پیلتایر (Peltier, 2016) سیستم‌های اطلاعاتی در کتابخانه‌ها ارائه خدمات و مجموعه‌ها را از طریق اینترنت برای مشتریان درون سازمانی و برون سازمانی فراهم نموده که همین دسترس‌پذیری از طریق اینترنت این سیستم‌ها را با خطرات امنیتی مواجه ساخته است. از آنجا که اطلاعات تجارت اصلی یک کتابخانه است لذا اطلاعات ارائه‌شده در سیستم‌های اطلاعاتی به منظور محافظت تهاجم‌های احتمالی نیازمند کنترل منسجم می‌باشند. کتابخانه‌ها بایستی محرمانه‌بودن دارایی‌های اطلاعاتی شان را از قبیل اطلاعات مالی کتابخانه، اطلاعات گردش مالی مشتریان، رمز عبور برای دسترسی به سیستم‌های اطلاعاتی کتابخانه و سایر موارد را حفظ کنند. مشتریان نیز بایستی دسترسی تأییدشده‌ای به رایانه‌های کتابخانه، وب‌سایت‌ها، پایگاه‌های اطلاعاتی و شبکه‌ها داشته باشند. لذا از آنجا که امنیت اطلاعات نقش بسیار مهمی در حمایت از

1. Security Thread

فعالیت‌های سازمان‌ها دارد، نیاز به یک استاندارد یا معیاری که نظارت بر امنیت اطلاعات را سامان دهد ضروری است (ملک الکلامی، ۱۳۹۲).

از آنجایی که هزینه‌های گزافی صرف تهیه و خرید منابع و پایگاه‌های اطلاعاتی در کتابخانه‌های دیجیتالی می‌شود لذا حفظ و نگهداری از اطلاعات از جنبه‌های مهم و ضروری کتابخانه‌هاست (میردامادی، ۱۳۸۷). در میان انواع کتابخانه‌ها، کتابخانه‌های دیجیتالی که بخشی از نظام آموزشی کشور هستند به‌عنوان مراکز تأمین و اشاعه اطلاعات تخصصی برای جامعه علمی دارای اهمیت قابل توجهی می‌باشند (مؤسسه استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷). باتوجه‌به اینکه حفظ و نگهداری اطلاعات در کتابخانه‌های دیجیتالی مانند سایر سازمان‌ها از اهمیت زیادی برخوردار است و به‌دلیل صرف هزینه‌های بسیار برای این دارایی و خرید پایگاه‌های اطلاعاتی مختلف در کتابخانه‌های دیجیتالی به‌نظر می‌رسد انجام چنین پژوهشی که وضعیت مدیریت امنیت اطلاعات را در کتابخانه‌های دیجیتالی روشن خواهد نمود و نیز نتایج آن در سیاست گذاری و برنامه ریزی مدیریت امنیت اطلاعات در این کتابخانه‌ها مؤثر خواهد بود، ضروری است. لذا از آنجایی که تاکنون پژوهشی درباره ارائه الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی انجام نگرفته، پژوهشگر درصدد است که به طراحی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی پرداخته شود.

با بررسی مطالعات انجام‌شده در حوزهٔ مدیریت امنیت اطلاعات مشخص شد که تحقیقات کمی در این زمینه انجام شده است. افزون‌براین، ارائهٔ مدل مدیریت امنیت اطلاعات به سابقهٔ آن مرتبط نیست. در زیر به تحقیقاتی اشاره می‌شود که با بعدی از ابعاد موضوع تحقیق در ارتباط هستند. مطالعات انجام‌گرفته در جدول شمارهٔ ۱ همراه روش‌های تحلیل و نتایج به‌دست‌آمده خلاصه شده است.

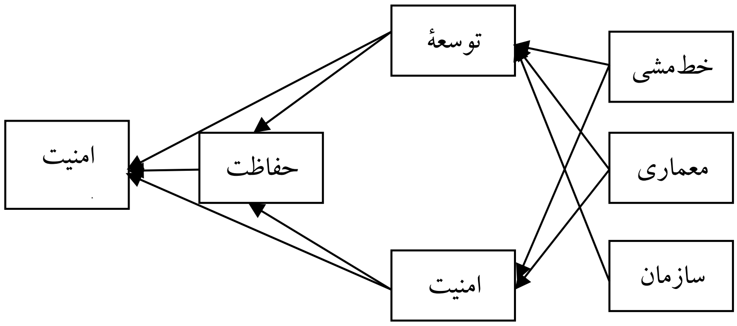
**جدول ۱. پیشینهٔ پژوهش‌های انجام‌گرفته**

| محققین | سال | عنوان تحقیق | جامعهٔ مطالعه‌شده | نتایج |
|---|---|---|---|---|
| آرام | ۱۳۸۸ | بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات | شرکت گاز پارس جنوبی | نتایج پژوهش حاکی از تأثیرگذاری بیشتر عوامل انسانی از دیدگاه کارشناسان فناوری اطلاعات بود و پس از آن شاخص‌های مربوط به عوامل مدیریتی، فنی و مالی قرار داشت. |
| زنده‌دل نوبری | ۱۳۸۹ | ارائهٔ مدلی جهت رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها | سازمان‌های شهر تهران | باتوجه‌به یافته‌ها، از نظر بلوغ امنیت، بانک پاسارگارد رتبهٔ اول، دانشگاه تهران رتبهٔ دوم و بانک تجارت رتبهٔ سوم را به‌دست آوردند. |
| ملک الکلامی | ۱۳۹۰ | ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در | کتابخانه‌های مرکزی دانشگاه‌های دولتی | نتایج پژوهش حاکی از آن است که به‌طورکلی کتابخانه‌های مرکزی دانشگاه‌های |

| محققین | سال | عنوان تحقیق | جامعهٔ مطالعه‌شده | نتایج |
|---|---|---|---|---|
| | | کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران براساس استاندارد بین‌المللی ایزو/ آی.ای.سی.۲۷۰۰۲ | مستقر در شهر تهران | دولتی مستقر در شهر تهران از لحاظ مدیریت امنیت اطلاعات در شرایط مطلوبی قرار دارند و با اطمینان ۹۵٪ می‌توان گفت، میانگین مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد ایزو آی. ای. سی. ۲۷۰۰۲ برابر با ۴ بوده و بالاتر از حد متوسط است و در سطح مطلوبی قرار دارد. |
| نورایی | ۱۳۹۱ | بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعات ISMS در ایران | بانک دی | یافته‌های این تحقیق حاکی از تأیید اثرگذاری استقرار سیستم مدیریت امنیت اطلاعات روی متغیرهای محرمانگی، یکپارچگی، دسترس‌پذیری، صحت و جواب‌گویی اطلاعات |
| باغبان‌زاده | ۱۳۹۳ | شناسایی و اولویت‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات | توزیع برق استان یزد | نتایج نشان داد که پنج شاخص اول به شرح زیر هستند:<br>• اشاعه و استفاده از اطلاعات محرمانه (امنیتی)<br>• سوءاستفاده از سیستم اطلاعات (سوء استفادهٔ عمدی کارمندان داخلی از منابع IS)<br>• آگاهی از اهمیت و ضرورت پیروی از قوانین و اجرای فعالیت‌های امنیتی<br>• استفاده از ابزارهای آموزشی متنوع برای آموزش فعالیت‌های مرتبط با امنیت سیستم‌های اطلاعاتی<br>• تعهد و وفاداری کارمندان به سازمان و حفظ اطلاعات<br>• درنهایت با نظرسنجی از خبرگان و پیشینهٔ تحقیق، راهکارهای بهبود امنیت اطلاعات که باتوجه‌به شاخص‌های برتر و تأثیرگذار در این شرکت ارائه گردید. این راهکارها عبارت‌اند از:<br>• پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات نظیر سیستم مدیریت امنیت فناوری اطلاعات<br>• ISO270007 استفاده از سیستم‌ها و نرم‌افزارهایی در جهت محدودکردن دسترسی کاربران به اطلاعات<br>• برگزاری دوره‌های آموزشی ضمن خدمت برای کارکنان جهت آشنایی با اصول امنیت اطلاعات در سازمان و آگاه‌کردن کارمندان از اهمیت و |

| محققین | سال | عنوان تحقیق | جامعهٔ مطالعه‌شده | نتایج |
|---|---|---|---|---|
| | | | | ضرورت آن<br>• وجود افراد آموزش دیده و متخصص در زمینه امنیت اطلاعات و سیستم‌ها |
| ارنست چانگ و هو | ۲۰۰۶ | اثربخشی عوامل سازمانی بر مدیریت امنیت اطلاعات | کارکنان سازمان | براساس یافته‌های پژوهش، توانایی مدیران فناوری اطلاعات و نبود اطمینان محیطی، تأثیر مثبتی روی سازمان‌ها در پیاده‌سازی مدیریت امنیت اطلاعات و استاندارد BS7799داشته است. همچنین یافته‌ها نشان داد، عوامل سازمانی چون اندازهٔ سازمان و نوع صنعت، به نحو چشمگیری کاربرد مدیریت امنیت اطلاعات را تحت تأثیر قرار می‌دهد. |
| کوزما | ۲۰۱۰ | کتابخانه‌های دیجیتال اروپایی: آسیب پذیری‌های امنیتی وب | کتابخانه‌های دیجیتالی اروپا | نتایج نشان داد، اکثر کتابخانه‌های دیجیتالی نقص امنیتی جدی در برنامه‌های کاربردی تحت وب خود دارند. اکثر کتابخانه‌های اروپای غربی، مشکلات امنیتی بحرانی (۵۱٪) یا در سطح متوسط (۱۰٪) داشتند که منجربه تجارت ناامن آنلاین شده بود. همچنین یافته‌ها حاکی از این بود که باوجود قوانین مربوط به حفاظت اطلاعات، کتابداران اقدام‌های لازم برای ایمن‌سازی سیستم‌های اطلاعاتی آنلاین را اجرا نمی‌کنند. |
| تینتاماسیک | ۲۰۱۳ | بررسی ارتباط سیستم‌های سازمان و آگاهی از امنیت اطلاعات | کارکنان سازمان | بر اساس یافته‌ها، ارتباط معناداری بین آگاهی کاربران از امنیت اطلاعات و ابعاد ساختار سازمان رسمی، ابعاد فرهنگ سازمانی و روش‌ها و سیاست‌های منابع انسانی وجود دارد. |

براساس مرور تحقیقات قبلی مشخص شد که اکثر تحقیقات انجام‌شده به عوامل مؤثر بر مدیریت امنیت اطلاعات پرداخته‌اند و تا حالا تحقیقی که به طراحی و صورت‌بندی مدلی در زمینهٔ امنیت اطلاعات بپردازد، وجود نداشته است. باتوجه‌به چهارچوب نظری به‌دست‌آمده از پیشینهٔ پژوهشی، مدل مفهومی پژوهش در شکل ۱ ترسیم شد.




**شکل۱. مدل مفهومی پژوهش**

همان‌طور که ملاحظه می‌شود، در این مدل متغیرهای سازمان‌دهی امنیت اطلاعات، معماری اطلاعات و خط‌مشی امنیت اطلاعات به‌عنوان متغیرهای مستقل، توسعهٔ سیستم‌های اطلاعاتی و حفاظت محتوا به‌عنوان متغیرهای میانجی و امنیت اطلاعات در کتابخانه‌های دیجیتالی به‌عنوان متغیر وابسته در نظر گرفته شده‌اند. بنابراین فرضیه‌های پژوهش حاضر به‌صورت زیر طرح شد:

**فرضیهٔ ۱:** خط‌مشی امنیت اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی تأثیر مثبت دارد.

یکی از متغیرهای تأثیرگذار بر توسعهٔ سیستم‌های اطلاعاتی، خط‌مشی امنیت اطلاعات است. کوزما (Kuzma,2010) معتقد است، درواقع، خط‌مشی‌های مدیریتی، راهنمایی برای به‌روزرسانی، نظارت‌کردن، تهیهٔ نسخ پشتیبان و بازرسی‌کردن در یک سازمان هستند. خط‌مشی‌ها باید به اندازه‌ای واضح و روشن باشند که بتوانند به کارکنان مدیریتی امکان تمرکز روی سیستم‌های اطلاعاتی را فراهم کنند. دراین‌میان، سیاست باید به نحوی انعطاف‌پذیر باشد که در آن مشکل‌های اورژانسی و پیش‌بینی نشده نیز گنجانده شود.

**فرضیهٔ ۲:** معماری اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی تأثیر مثبت دارد.

قانون کلینگرکوهن تصریح دارد، معماری اطلاعات برای ارتقا یا نگهداری فناوری موجود و کسب فناوری اطلاعاتی جدید درجهت رسیدن‌به اهداف راهبردی سازمان و مدیریت منابع آن چهارچوبی یکپارچه فراهم می‌کند. معماری اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی تأثیر می‌گذارد. کتابخانه‌ها وظیفه دارند، قدرت فزایندهٔ سیستم‌های اطلاعاتی ساختارمند را که مدت‌ها به‌عنوان جزئی از کتابخانه‌ها مطرح بوده‌اند، مهارکرده و این سیستم‌ها را در کانال‌های جدیدی که تأمین‌کنندهٔ نیازها و اهداف کاربران باشد، به‌کاربرند. این چالش به‌وسیلهٔ توسعهٔ سیستم‌های جدید و استانداردهای فنی پاسخ داده می‌شود. در این زمینه، معماری اطلاعات نقش اصلی را ایفا می‌کند.

**فرضیهٔ ۳:** سازمان‌دهی امنیت اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی تأثیر مثبت دارد.

«سازماندهی امنیت اطلاعات» به‌عنوان متغیری اثرگذار بر توسعهٔ سیستم‌های اطلاعاتی، عامل اصلی تأثیرگذار بر توان سازمان در حفاظت از امنیت اطلاعات است. علاوه‌براین، یکی از مهم‌ترین توانمندسازها در هدایت و مدیریت اثربخش امنیت اطلاعات نیز هست. در حوزهٔ مدیریت و امنیت اطلاعات، برای تحقق تعدادی از اهداف باید ابزارهای لازم (توانمندسازها) را در اختیار داشت. سازماندهی باعث کاهش اتلاف منابع سازمان می‌شود. بانگاهی گذرا به سازمان می‌توان به این موضوع پی‌برد که به‌واسطهٔ تصمیم‌گیری‌های اشتباه چقدر زمان، هزینه و تلاش سازمان صرف رفع تعارضات و تداخلات ناشی از ضعف سازماندهی می‌شود. این خود گویای اهمیت موضوع نزد صاحبان اندیشه است.

**فرضیهٔ ٤:** خط‌مشی امنیت اطلاعات بر امنیت منابع انسانی تأثیر مثبت دارد.

یکی از متغیرهای تأثیرگذار بر امنیت منابع انسانی خط‌مشی امنیت اطلاعات است. هدف خط‌مشی امنیت اطلاعات، جهت‌دادن به پیاده‌سازی امنیت اطلاعات است. برنامه چهارچوبی را برای اهداف در جهت الزام به محرمانگی، جامعیت و دردسترس‌بودن فراهم می‌آورد. موفقیت امنیت اطلاعات تا حدزیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حدزیادی بالا ببرد؛ درحالی‌که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود.

**فرضیهٔ ٥:** معماری اطلاعات بر امنیت منابع انسانی تأثیر مثبت دارد.

معماری اطلاعات یکی از متغیرهای تأثیرگذار بر امنیت منابع انسانی است. وان سولمز( Von Solms, 2004) معتقد است که معماری اطلاعات در مؤلفه‌های منابع انسانی نقش به‌سزایی دارد. شاخص‌های مؤثر در امنیت نیروی انسانی که می‌توانند سبب بروز اختلال در فعالیت‌های نیروی انسانی می‌شوند عبارتند از: کار زیاد، نداشتن مهارت کافی و لازم، تداخل مسئولیت‌ها، اطلاع‌نداشتن از میزان ارزش اطلاعات، نداشتن انگیزه، کوتاهی و بی‌مسئولیتی و فراموش کاری. یکی از جنبه‌های مهم و اثرگذار معماری اطلاعات است که می‌تواند شاخص‌های مذکور را تعدیل کند.

**فرضیهٔ ٦:** سازمان‌دهی امنیت اطلاعات بر امنیت منابع انسانی تأثیر مثبت دارد.

سازماندهی عاملی اصلی و تأثیرگذار بر توان سازمان در امنیت منابع انسانی است. ویتمن (Wheatman, 2010) معتقد است که سازماندهی تأثیر مستقیمی در اجرای موفق و مؤثر برنامه‌های امنیتی سازمان دارد. به این معنا که هرچقدر «سازماندهی امنیت اطلاعات» یک سازمان منسجم‌تر باشد، قطعاً می‌توان به اجرای موفق برنامه‌های امنیت اطلاعات در سازمان امیدوارتر بود. تدوین برنامه و صرف‌کردن

هزینه، شرط لازم برای رسیدن به اهداف است؛ اما بدون وجود ساختاری مناسب برای اجرای برنامه‌ها، تحقق اهداف، دور از دسترس بوده یا با هزینه‌های گزافی صورت می‌پذیرد. بنابراین یکی از عوامل اصلی توفیق برنامه‌ها، به‌خصوص برنامه‌های امنیتی، سازماندهی اثربخش امنیت اطلاعات است.

**فرضیۀ ۷:** توسعۀ سیستم‌های اطلاعاتی بر حفاظت محتوا تأثیر مثبت دارد.

یکی از متغیرهای تأثیرگذار بر حفاظت اطلاعات، توسعۀ سیستم‌های اطلاعاتی است.اسچویو (Schou, 2004) معتقد است، توسعۀ سیستم اطلاعاتی در سازمان، مجموعه‌ای از عناصر وابسته به هم است که وظیفۀ جمع‌آوری، پردازش، ذخیره‌سازی و توزیع اطلاعات به‌منظور پشتیبانی از تصمیم‌گیری، کنترل و هماهنگی بین بخش‌های مختلف را در سازمان بر عهده دارد. سیستم اطلاعاتی می‌تواند به مدیران و کارکنان در تحلیل مشکلات، تجسم بهتر و تصویرکردن موضوعات پیچیده و همچنین در تولید محصولات جدید کمک کند. همچنین سیستم‌های اطلاعاتی، اطلاعات مربوط‌به افراد، مکان‌ها و هر جز تصورکردنی از داخل و خارج سازمان را در خود ذخیره و حفاظت می‌کنند.

**فرضیۀ ۸:** توسعۀ سیستم‌های اطلاعاتی بر امنیت اطلاعات در کتابخانه‌های دیجیتالی تأثیر مثبت دارد.

توسعۀ سیستم‌های اطلاعاتی بر امنیت اطلاعات تأثیر می‌گذارد. بایس (Baise, 2006) به چهار موج امنیت اطلاعات پرداخته است. موج اول، فنی بود. که به راه‌حل‌های فنی ارائه‌شده برای مسائل امنیتی مربوط می‌شد. موج دوم، به بعد مدیریتی قوی امنیت اطلاعات می‌پردازد. این ابعاد مانند خط‌مشی و درگیری مدیریت بسیار مهم هستند. موج سوم، از یک نیاز برای داشتن فرمی از استانداردکردن امنیت اطلاعات در شرکت و جنبه‌هایی مانند بهترین ریتم‌های مدیریتی، تأیید یک فرهنگ مناسب امنیت اطلاعات و اندازه‌گیری و نظارت امنیت اطلاعات تشکیل شده است. موج چهارم نیز دربارۀ توسعۀ نقش قطعی چگونگی ادارۀ امنیت اطلاعات است.

**فرضیۀ ۹:** امنیت منابع انسانی بر حفاظت محتوا تأثیر مثبت دارد.

گونزالز و ساویکا (Gonzalez & Sawicka,2002) عامل انسانی را به‌عنوان پاشنۀ آشیل امنیت اطلاعات معرفی و بیان کرد که سال ۲۰۰۶، حملات کوچک‌تر، متمرکزتر و پنهان‌کارانه‌تری به سیستم‌های اطلاعاتی سازمان‌ها صورت خواهد گرفت. کانون توجه نفوذگران ، «سهل‌انگاری و ساده‌اندیشی کاربران» خواهد بود.

**فرضیۀ ۱۰:** امنیت منابع انسانی بر امنیت اطلاعات در کتابخانه‌های دیجیتالی تأثیر مثبت دارد.

امنیت منابع انسانی بر امنیت اطلاعات در سازمان تأثیر دارد. یکی از مؤلفه‌های مهم در مدیریت امنیت اطلاعات در سازمان توجه‌به امنیت از منظر منابع انسانی است. به‌طوری‌که بدون در نظرگرفتن عوامل انسانی راه‌حل‌های فنی چندان تأثیری در مدیریت امنیت اطلاعات نخواهند داشت.

**فرضیهٔ ۱۱:** حفاظت اطلاعات بر امنیت اطلاعات در کتابخانه‌های دیجیتالی تأثیر مثبت دارد.

یکی از متغیرهای تأثیرگذار بر امنیت اطلاعات در کتابخانه‌های دیجیتالی، حفاظت اطلاعات است. برینی (Briney, 2001) معتقد است که نحوهٔ استفاده و کنترل دستیابی به منابعی که به اشتراک گذاشته شده‌اند، از مهمترین هدف‌های سیستم امنیتی در شبکه است. هر سازمان برای حفاظت از اطلاعات ارزشمند، باید به راهبرد خاصی پایبند باشد و براساس آن سیستم امنیتی را پیاده‌سازی و اجرا نماید.

## روش‌شناسی

روش اجرای پژوهش حاضر توصیفی‌پیمایشی و طرح پژوهش همبستگی از نوع تحلیل مسیر است؛ زیرا در این پژوهش، روابط بین متغیرها در قالب الگوی علّی بررسی می‌شود. جامعهٔ آماری پژوهش، کارشناسان و کتابداران کتابخانه‌های دیجیتالی دانشگاه‌های شهر تهران است. براساس اطلاعات به‌دست‌آمده، به‌صورت تقریبی، ۴۰۰ نفر در این کتابخانه‌ها مشغول به‌کار هستند. بااستفاده از فرمول کوکران، ۱۹۶ نفر به‌عنوان نمونه و به‌صورت هدفمند انتخاب و پرسش‌نامهٔ پژوهش بین آن‌ها توزیع شد. از ۱۹۶ پرسش‌نامه، ۱۹۰تا پاسخ داده شد. درنهایت، ۱۹۰ پرسش‌نامه وارد تحلیل شدند. برای اطمینان از روایی ابزارهای اندازه‌گیری، تحلیل عاملی تأییدی بااستفاده از نرم‌افزار لیزرل[1] انجام شد. تحلیل عاملی تأییدی مشخص می‌کند که کدام متغیرها با کدام عامل‌ها و کدام عامل‌ها با کدام عامل‌ها همبسته می‌شود (کلاین[2]، ۲۰۰۵). درواقع، بااستفاده‌از این آزمون مشخص می‌شود، هریک از متغیرهای مشاهده‌شدهٔ پژوهش بارعاملی معناداری روی سازهٔ زیربنایی خود دارد یا خیر. یافته‌های مربوط به تحلیل عاملی تأییدی در جدول شماره ۲ درج شده است. این یافته‌ها حاکی از آن است که گویه‌های مربوط‌به متغیرهای خط‌مشی امنیت اطلاعات، توسعهٔ سیستم‌های اطلاعاتی، معماری اطلاعات، سازمان‌دهی امنیت اطلاعات، حفاظت اطلاعات و امنیت اطلاعات در کتابخانه‌های دیجیتالی به‌ترتیب بارهای عاملی پذیرفتنی دارند. همهٔ این بارهای عاملی در سطح آلفای $P<۰/۰۱$ معنادار هستند.

1. LISREL
2. Kline

**جدول۲. یافته‌های تحلیل عاملی تأییدی (تمامی بارهای عاملی در سطح آلفای ۰/۰۱ معنادار هستند)**

| متغیرها | آلفای کرونباخ | بارهای عاملی رو سازه‌ها | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | خط‌مشی امنیت اطلاعات | توسعهٔ سیستم‌های اطلاعاتی | معماری اطلاعات | سازمان‌دهی امنیت اطلاعات | امنیت منابع انسانی | حفاظت اطلاعات | امنیت اطلاعات |
| خط‌مشی امنیت اطلاعات | ۰/۸۹ | | | | | | | |
| P 1 | | ۰/۵۶ | | | | | | |
| P 2 | | ۰/۶۲ | | | | | | |
| P 3 | | ۰/۷۷ | | | | | | |
| توسعهٔ سیستم‌های اطلاعاتی | ۰/۸۲ | | | | | | | |
| DS 1 | | | ۰/۵۹ | | | | | |
| DS 2 | | | ۰/۷۲ | | | | | |
| DS 3 | | | ۰/۷۹ | | | | | |
| DS 4 | | | ۰/۸۱ | | | | | |
| DS 5 | | | ۰/۶۵ | | | | | |
| معماری اطلاعات | ۰/۸۷ | | | | | | | |
| A 1 | | | | ۰/۶۹ | | | | |
| A 2 | | | | ۰/۷۱ | | | | |
| A 3 | | | | ۰/۷۸ | | | | |
| A 4 | | | | ۰/۶۶ | | | | |
| A 5 | | | | ۰/۷۸ | | | | |
| سازمان‌دهی امنیت اطلاعات | ۰/۹۱ | | | | | | | |
| O 1 | | | | | ۰/۷۵ | | | |
| O 2 | | | | | ۰/۶۵ | | | |
| O 3 | | | | | ۰/۸۵ | | | |
| O 4 | | | | | ۰/۸۳ | | | |
| امنیت منابع انسانی | ۰/۸۸ | | | | | | | |
| HR 1 | | | | | | ۰/۸۱ | | |
| HR 2 | | | | | | ۰/۷۸ | | |
| HR 3 | | | | | | ۰/۶۹ | | |
| HR 4 | | | | | | ۰/۷۱ | | |

| متغیرها | آلفای کرونباخ | بارهای عاملی رو سازه‌ها | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | خط‌مشی امنیت اطلاعات | توسعهٔ سیستم‌های اطلاعاتی | معماری اطلاعات | سازمان‌دهی امنیت اطلاعات | امنیت منابع انسانی | حفاظت اطلاعات | امنیت اطلاعات |
| حفاظت اطلاعات | ۰/۸۲ | | | | | | | |
| S 1 | | | | | | | ۰/۷۰ | |
| S 2 | | | | | | | ۰/۶۹ | |
| S 3 | | | | | | | ۰/۶۲ | |
| امنیت اطلاعات در کتابخانه‌های دیجیتالی | ۰/۸۹ | | | | | | | |
| IS 1 | | | | | | | | ۰/۶۸ |
| IS 2 | | | | | | | | ۰/۷۵ |
| IS 3 | | | | | | | | ۰/۶۳ |
| IS 4 | | | | | | | | ۰/۸۲ |

همچنین نتایج به‌دست‌آمده نشان می‌دهد که هریک از سازه‌های خط‌مشی امنیت اطلاعات، معماری اطلاعات، سازمان‌دهی امنیت اطلاعات، توسعهٔ سیستم‌های اطلاعاتی، امنیت منابع انسانی و حفاظت محتوا و امنیت اطلاعات در کتابخانه‌های دیجیتالی شاخص‌های برازش پذیرفتنی است.

خط‌مشی امنیت اطلاعات: برای اندازه‌گیری خط‌مشی امنیت اطلاعات از پرسش‌نامهٔ محقق‌ساخته استفاده شد. این پرسش‌نامه از سه گویه تشکیل شده است. سؤالات براساس طیف پنج‌درجه‌ای لیکرت اندازه‌گیری شدند. به‌طوری‌که در این طیف کاملاً مخالفم، درجهٔ یک و به‌ترتیب، کاملاً موافقم درجهٔ پنج گرفته است. ضریب همسانی درونی این پرسش‌نامه با استفاده از آلفای کرونباخ ۰/۸۹ به‌دست آمد. همچنین شاخص‌های به‌دست‌آمده از تحلیل عامل تأییدی GFI=۰/۹۲، RMSEA= ۰/۰۴۷، AGFI= ۰/۹۰ نشان از برازندگی مناسب الگو با داده‌ها دارد.

توسعهٔ سیستم‌های اطلاعاتی: پرسش‌نامهٔ توسعهٔ سیستم‌های اطلاعاتی با چهار گویه تدوین و براساس مقیاس پنج‌درجه‌ای لیکرت درجه‌بندی شده است. مقیاس لیکرت نوعی مقیاس فاصله‌ای است که از پنج‌درجهٔ کاملاً مخالفم، مخالفم، نظری ندارم، موافقم و کاملاً موافقم بهره می‌گیرد. ضریب همسانی درونی این پرسش‌نامه با استفاده از روش آلفای کرونباخ ۰/۸۲ به‌دست آمد. همچنین شاخص‌های تحلیل عامل تأییدی GFI=۹۳، AGFI=۰/۹۲، RMSEA=۰/۰۲۸ نشان می‌دهد که الگو با داده‌ها برازش مناسبی دارد.

معماری اطلاعات: برای اندازه‌گیری معماری اطلاعات از پرسش‌نامه محقق‌ساخته استفاده شد. این پرسش‌نامه از پنج‌گویه تشکیل شده است. این پرسش‌نامه براساس طیف پنج‌درجه‌ای لیکرت (درجهٔ یک برای کاملاً مخالفم تا درجهٔ پنج برای کاملاً موافقم) نمره‌گذاری می‌شود. ضریب همسانی درونی این پرسش‌نامه با استفاده از روش آلفای کرونباخ ۰/۸۷ به‌دست آمد. همچنین شاخص‌های تحلیل عامل تأییدی برای بررسی روایی GFI=۹۷، AGFI=۰/۹۴، RMSEA=۰/۰۴۷ نشان می‌دهد که الگو با داده‌ها برازش مناسبی دارد.

سازمان‌دهی امنیت اطلاعات: برای اندازه‌گیری سازمان‌دهی امنیت اطلاعات از پرسش‌نامهٔ محقق‌ساخته استفاده شد. این پرسش‌نامه از چهار گویه تشکیل شده است. سؤالات براساس طیف پنج‌درجه‌ای لیکرت (درجهٔ یک برای کاملاً مخالفم تا درجهٔ پنج برای کاملاً موافقم) اندازه‌گیری شدند. ضریب همسانی درونی این پرسش‌نامه با استفاده از آلفای کرونباخ ۰/۹۱ به‌دست آمد. همچنین شاخص‌های به‌دست‌آمده از تحلیل عامل تأییدی GFI=۰/۹۸، RMSEA=۰/۰۴۵، AGFI=۰/۹۷ نشان از برازندگی مناسب الگو با داده‌ها دارد.

امنیت منابع انسانی: برای اندازه‌گیری امنیت منابع انسانی از پرسش‌نامهٔ محقق‌ساخته استفاده شد. این پرسش‌نامه از چهار گویه تشکیل شده است. این پرسش‌نامه بر اساس طیف پنج‌درجه‌ای لیکرت (درجهٔ یک برای کاملاً مخالفم تا درجهٔ پنج برای کاملاً موافقم) نمره‌گذاری می‌شود. ضریب همسانی درونی این پرسش‌نامه با استفاده از روش آلفای کرونباخ ۰/۸۷ به‌دست آمد. همچنین شاخص‌های تحلیل عامل تأییدی برای بررسی روایی GFI=۰/۹۶، AGFI=۱، RMSEA=۰/۰۶۴ نشان می‌دهد که الگو با داده‌ها برازش مناسبی دارد.

حفاظت اطلاعات: پرسش‌نامهٔ حفاظت اطلاعات با ۳ گویه تدوین شده است و براساس مقیاس پنج‌درجه‌ای لیکرت درجه‌بندی شده است.مقیاس لیکرت نوعی مقیاس فاصله‌ای است که به‌ویژه از پنج‌درجهٔ کاملاً مخالفم، مخالفم، نظری ندارم، موافقم و کاملاً موافقم بهره می‌گیرد. ضریب همسانی درونی این پرسش‌نامه با استفاده از روش آلفای کرونباخ ۰/۸۲ به‌دست آمد. همچنین شاخص‌های تحلیل عامل تأییدی GFI=۹۵، AGFI=۰/۹۵، RMSEA=۰/۰۷۱ نشان می‌دهد که الگو با داده‌ها برازش مناسبی دارد.

امنیت اطلاعات در کتابخانه‌های دیجیتالی: برای اندازه‌گیری امنیت اطلاعات در کتابخانه‌های دیجیتالی از پرسش‌نامهٔ محقق‌ساخته استفاده شد. این پرسش‌نامه از ۴ گویه تشکیل شده است. این

پرسش‌نامه بر اساس طیف پنج‌درجه‌ای لیکرت (درجهٔ یک برای کاملاً مخالفم تا درجهٔ پنج برای کاملاً موافقم) نمره‌گذاری می‌شود. ضریب همسانی درونی این پرسش‌نامه با استفاده از روش آلفای کرونباخ ۰/۸۹ به‌دست آمد. همچنین شاخص‌های تحلیل عامل تأییدی برای بررسی روایی GFI=۹۷، AGFI=۰/۹۴، RMSEA=۰/۰۴۷ نشان می‌دهد که الگو با داده‌ها برازش مناسبی دارد.

برای تجزیه و تحلیل داده‌ها از روش الگوی معادلات ساختاری استفاده شد. مدل معادلات ساختاری یا به‌طور اختصار SEM، از روش‌های جدید آماری و یکی از قوی‌ترین روش‌های تجزیه و تحلیل چندمتغیره است که برخی هم به آن تحلیل ساختاری کواریانس و الگوسازی علی اطلاق می‌کنند. کاربرد اصلی آن در موضوعات چند متغیری است که نمی‌توان آن‌ها را به‌شیوهٔ دو متغیری با درنظرگرفتن هربار یک متغیر مستقل با یک متغیر وابسته انجام داد. تجزیه و تحلیل چندمتغیره به روش‌های تجزیه و تحلیلی اطلاق می‌شود که ویژگی اصلی آن‌ها، تجزیه و تحلیل همزمان چند متغیر مستقل با چند متغیر وابسته است.

## یافته‌ها

یافته‌های مربوط به متغیرهای جمعیت‌شناختی پژوهش در جدول ۴ درج شده است. یافته‌ها نشان می‌دهد که ۷۲/۲درصد پاسخ‌دهندگان را مردان و ۲۷/۸درصد پاسخ‌گویان را زنان تشکیل می‌دهند. در زمینهٔ توزیع فراوانی پاسخ‌هندگان بر حسب متغیر سن یافته‌های پژوهش حاکی از آن بود که ۴۲/۱درصد از پاسخ‌دهندگان در سن ۲۵ تا ۳۱ سال، ۳۴/۲درصد در سنین بین۳۱ تا ۳۵ سال، ۱۸/۴درصد در سن ۳۶ تا ۴۰ سال، ۵/۲درصد در سن بالاتر از ۴۱ سال قرار داشتند.

**جدول٤. یافته‌های جمعیت شناختی پژوهش**

| متغیرها | فراوانی | درصد فراوانی |
|---|---|---|
| جنس | | |
| مرد | ۱۳۷ | ۷۲/۲ |
| زن | ۵۳ | ۲۷/۸ |
| سن | | |
| ۲۵ تا ۳۱ سال | ۸۰ | ۴۲/۱ |
| ۳۱ تا ۳۵ سال | ۶۵ | ۳۴/۲ |
| ۳۶ تا ۴۰ سال | ۳۵ | ۱۸/۴ |
| ۴۱ سال به بالا | ۱۰ | ۵/۲ |

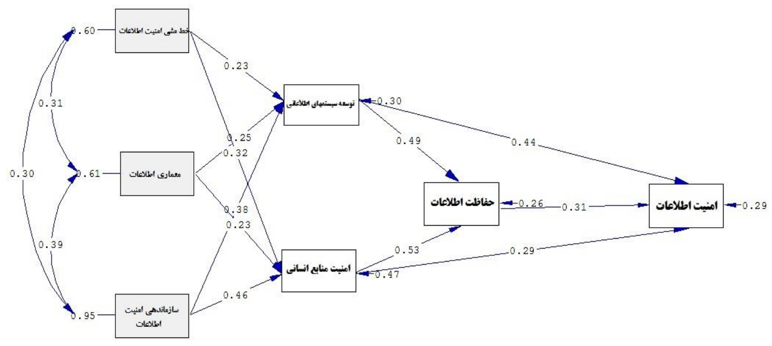
پس از محاسبهٔ شاخص‌های توصیفی متغیرهای پژوهش، به‌منظور بررسی روابط علّی بین متغیرها از روش الگوی معادلات ساختاری استفاده شد. باتوجه‌به اینکه مبنای تجزیه و تحلیل الگوهای علّی، ماتریس همبستگی است، ماتریس همبستگی، میانگین و انحراف معیار متغیرهای بررسی‌شده، در جدول ۵ ارائه می‌شود.

**جدول ۵. ماتریس همبستگی متغیرهای پژوهش ($P^{*}$<۰/۰۵ و $P^{**}$<۰/۰۱)**

| متغیرها | خط‌مشی امنیت اطلاعات | توسعهٔ سیستم‌های اطلاعاتی | معماری اطلاعات | سازمان‌دهی امنیت اطلاعات | امنیت منابع انسانی | حفاظت اطلاعات | امنیت اطلاعات |
|---|---|---|---|---|---|---|---|
| خط‌مشی امنیت اطلاعات | ۱ | | | | | | |
| توسعهٔ سیستم‌های اطلاعاتی | ۰/۶۸$^{**}$ | ۱ | | | | | |
| معماری اطلاعات | ۰/۵۱$^{**}$ | ۰/۶۲$^{**}$ | ۱ | | | | |
| سازمان‌دهی امنیت اطلاعات | ۰/۵۵$^{**}$ | ۰/۴۸$^{**}$ | ۰/۴۵$^{**}$ | ۱ | | | |
| امنیت منابع انسانی | ۰/۳۵$^{**}$ | ۰/۴۱$^{**}$ | ۰/۳۸$^{**}$ | ۰/۵۲$^{**}$ | ۱ | | |
| حفاظت اطلاعات | ۰/۴۳$^{**}$ | ۰/۳۹$^{**}$ | ۰/۵۸$^{**}$ | ۰/۴۲$^{**}$ | ۰/۵۷$^{**}$ | ۱ | |
| امنیت اطلاعات | ۰/۴۹$^{**}$ | ۰/۳۳$^{**}$ | ۰/۵۶$^{**}$ | ۰/۴۸$^{**}$ | ۰/۶۱$^{**}$ | ۰/۴۴$^{**}$ | ۱ |
| میانگین | ۳/۲۲ | ۳/۵۱ | ۳/۶۵ | ۳/۴۰ | ۳/۴۲ | ۳/۵۴ | ۳/۷۱ |
| انحراف معیار | ۰/۸۹ | ۱/۱۰ | ۱/۰۹ | ۱/۰۲ | ۱/۰۱ | ۰/۹۵ | ۱/۱۱ |

همان‌طورکه در جدول ۵ مشاهده می‌شود، از میان متغیرهای پژوهش به‌ترتیب امنیت منابع انسانی (r=۰/۶۱)، معماری اطلاعات (r= ۰/۵۶)، خط‌مشی امنیت اطلاعات (r= ۰/۴۹)، سازمان‌دهی امنیت اطلاعات (r= ۰/۴۸)

و توسعهٔ سیستم‌های اطلاعاتی (r۰/۳۳= ) بالاترین ضریب همبستگی با مزیت رقابتی را دارند و ضریب همبستگی بین متغیرها در سطح (P<۰/۰۱) مثبت و معنادار است و توسعهٔ سیستم‌های اطلاعاتی (r= ۰/۳۳) بالاترین ضریب همبستگی با مزیت رقابتی را دارند است.




Chi-Square=156.03, df=87, P-value=0.08585, RMSEA=0.064

**شکل شماره ۲. الگوی برازش‌شده پژوهش**

شکل ۲ الگوی برازش‌شدهٔ پژوهش را نشان می‌دهد. اعداد روی مسیرها، پارامترهای استاندارد شده‌اند. مطابق با شکل ۲، تمام مسیرها در سطح (P<۰/۰۱) معنادارند. درمیان متغیرهای موجود در الگو، توسعهٔ سیستم‌های اطلاعاتی بیشترین اثر مستقیم را بر امنیت اطلاعات کتابخانه‌های دیجیتالی (۰/۴۴) دارد.

ازآنجاکه هدف پژوهش حاضر بررسی ارائهٔ الگوی استراتژیک مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی به‌روش تحلیل مسیر است، در جدول ۶ ضرایب اثر مستقیم، اثر غیرمستقیم، اثر کل و سطح معناداری بین متغیرهای پژوهش آورده شده است.

**جدول۶. برآورد ضرایب استانداردشده اثر مستقیم، غیرمستقیم و کل الگو** ($P^{*}$<۰/۰۵ و $P^{**}$<۰/۰۱)

| مسیر | اثر مستقیم | اثر غیر مستقیم | اثر کل |
|---|---|---|---|
| به روی توسعهٔ سیستم‌های اطلاعاتی از: | | | |
| خط‌مشی امنیت اطلاعات | ۰/۲۳** | - | ۰/۲۳** |
| معماری اطلاعات | ۰/۲۵** | - | ۰/۲۵** |
| سازماندهی امنیت اطلاعات | ۰/۳۸** | - | /۳۸** |
| به روی امنیت منابع انسانی از: | | | |
| خط‌مشی امنیت اطلاعات | ۰/۳۲** | - | ۰/۳۲** |
| معماری اطلاعات | ۰/۲۳** | - | ۰/۲۳** |
| سازماندهی امنیت اطلاعات | ۰/۴۶** | – | ۰/۴۶** |
| به روی حفاظت محتوا از: | | | |
| خط‌مشی امنیت اطلاعات | - | ۰/۱۱** | ۰/۱۱** |
| معماری اطلاعات | – | ۰/۱۲** | ۰/۱۲** |

| مسیر | اثر مستقیم | اثر غیر مستقیم | اثر کل |
|---|---|---|---|
| سازماندهی امنیت اطلاعات | – | **۰/۱۸ | **۰/۱۸ |
| توسعهٔ سیستم‌های اطلاعاتی | **۰/۴۹ | – | **۰/۴۹ |
| امنیت منابع انسانی | **۰/۵۳ | – | **۰/۵۳ |
| به روی امنیت اطلاعات از : | | | |
| خط‌مشی امنیت اطلاعات | – | **۰/۱۷ | **۰/۱۷ |
| معماری اطلاعات | – | **۰/۱۶ | **۰/۱۶ |
| سازماندهی امنیت اطلاعات | – | **۰/۲۹ | **۰/۲۹ |
| توسعهٔ سیستم‌های اطلاعاتی | **۰/۴۴ | **۰/۱۵ | **۰/۵۹ |
| امنیت منابع انسانی | **۰/۲۹ | **۰/۱۶ | **۰/۴۵ |
| حفاظت اطلاعات | **۰/۳۱ | – | **۰/۳۱ |

همان‌طورکه در جدول ۶ مشاهده می‌شود، اثر مستقیم خط‌مشی امنیت اطلاعات ($\beta$ =۰/۲۳)، معماری اطلاعات ($\beta$=۰/۲۵) و سازماندهی امنیت اطلاعات ($\beta$ =۰/۳۸) بر توسعهٔ سیستم‌های اطلاعاتی در سطح (P<۰/۰۱) مثبت و معنادار است. اثرمستقیم خط‌مشی امنیت اطلاعات ($\beta$ =۰/۳۲)، معماری اطلاعات ($\beta$ =۰/۲۳) و سازماندهی امنیت اطلاعات ($\beta$ =۰/۴۶) بر امنیت منابع انسانی در سطح (P<۰/۰۱) مثبت و معنادار است. اثرمستقیم توسعهٔ سیستم‌های اطلاعاتی ($\beta$ =۰/۴۹) و امنیت منابع انسانی ($\beta$ =۰/۵۳) بر حفاظت اطلاعات در سطح (P<۰/۰۱) مثبت و معنادار است. همچنین اثرمستقیم توسعهٔ سیستم‌های اطلاعاتی ($\beta$ =۰/۴۴)، امنیت منابع انسانی ($\beta$ =۰/۲۹) و حفاظت اطلاعات ($\beta$ =۰/۳۱) بر امنیت اطلاعات در کتابخانه‌های دیجیتالی در سطح (P<۰/۰۱) مثبت و معنادار است.

**جدول ۷. مشخصه‌های برازندگی الگوی تحلیل مسیر**

| $\chi^2$/df | RMSEA | GFI | AGFI | CFI | NNFI |
|---|---|---|---|---|---|
| ۱/۷۹ | ۰/۰۶۴ | ۰/۹۵ | ۰/۹۷ | ۱ | ۰/۹۹ |

براساس جدول شماره۷ نسبت خی‌دو به درجهٔ آزادی ($\chi^2$/df=۱/۷۹) شاخص نکویی برازش (GFI=۰/۹۵)، شاخص تعدیل‌شدهٔ نکویی برازش (AGFI=۰/۹۷) و ریشهٔ خطای میانگین مجذورات تقریب (RMSEA=۰/۰۶۴) در سطح مناسبی هستند. بنابراین برازش الگوی برازش‌شده پژوهش در سطح مناسبی است.

## بحث و نتیجه‌گیری

هدف پژوهش حاضر، ارائهٔ الگوی استراتژیک مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی

با استفاده از تحلیل مسیر بود. نتایج تحلیل مسیر نشان داد، الگوی پیشنهادی با داده‌های این پژوهش برازش نسبتاً خوبی دارد. نتایج نشان داد که خط‌مشی امنیت اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی تأثیر مثبت و معناداری دارد. این یافته با نتایج پژوهش‌های (ملک الکلامی، ۱۳۹۰)، (نورایی، ۱۳۹۱)، کوزما (Kuzma, 2010)) و تینتاماسیک (Tintamusik, 2013) همخوانی دارد. در تبیین این یافته می‌توان گفت که اگر کتابخانه‌های دیجیتالی، اهداف و سیاست‌های امنیتی خود را تدوین کنند و در اختیار کارکنان قرار دهند و به‌صورت شفاف راهبردهای امنیت اطلاعات را اتخاذ و به‌کار گیرند، منجربه توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی در کتابخانه‌های دیجیتالی می‌شود.

نتایج نشان داد که معماری اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی تأثیر مثبت و معنادار دارد. این یافته با نتایج پژوهش‌های (زنده‌دل‌نوبری، ۱۳۸۹)، (ملک الکلامی ۱۳۹۰)، (نورایی، ۱۳۹۱)، کوزما (Kuzma, 2010) و تینتاماسیک (Tintamusik, 2013) همخوانی دارد. در تبیین این یافته می‌توان گفت که اطلاعات ممکن است باعث توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی شود، اگر که ساختار صحیحی در کتابخانه‌های دیجیتالی داشته باشند و چهارچوبی برای چیدمان اطلاعات تعریف شود تا کاربران به‌سرعت و سهولت به اطلاعات مدنظر خود دست یابد.

نتایج نشان داد که سازماندهی امنیت اطلاعات بر توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی تأثیر مثبت و معنادار دارد. این یافته با نتایج پژوهش‌های (ملک‌الکلامی، ۱۳۹۰)، (نورایی، ۱۳۹۱)، کوزما (Kuzma, 2010) و تینتاماسیک (Tintamusik, 2013 ) همخوانی دارد. این یافته نشان می‌دهد که اگر امنیت اطلاعات سازماندهی و مدیریت شود، سازماندهی باعث کاهش اتلاف منابع سازمان می‌شود. با نگاهی گذرا به سازمان می‌توان دریافت که به‌واسطهٔ تصمیم‌گیری‌های اشتباه، چقدر زمان، هزینه و تلاش سازمان صرف رفع تعارضات و تداخلات ناشی از ضعف سازماندهی می‌شود. ازاین‌رو، سازماندهی امنیت اطلاعات منجربه توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی می‌گردد. همچنین نتایج نشان داد، توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی بر حفاظت اطلاعات بر تأثیر مثبت و معنادار دارد. این یافته با نتایج پژوهش‌های (آرام، ۱۳۸۸)، (ملک‌الکلامی، ۱۳۹۰)، (نورایی، ۱۳۹۱)، ارنست چانگ و هو (Ernest Chang & Ho, 2006)، کوزما (Kuzma, 2010) و تینتاماسیک (Tintamusik, 2013) همخوانی دارد. توسعهٔ سیستم اطلاعاتی می‌تواند به مدیران و کارکنان در تحلیل مشکلات، تجسم بهتر و تصویرکردن موضوعات پیچیده و همچنین در تولید محصولات جدید کمک کند. همچنین سیستم‌های اطلاعاتی، اطلاعات مربوط‌به افراد، مکان‌ها و هر جزء تصورکردنی از داخل و خارج سازمان را در خود

ذخیره می‌کنند و در حفاظت اطلاعات نقش به‌سزایی دارد. هچنین امنیت منابع انسانی و رضایت آنها نیز در حفاظت اطلاعات نقش دارد.

همچنین نتایج نشان داد، توسعهٔ سیستم‌های اطلاعاتی و امنیت منابع انسانی بر امنیت اطلاعات کتابخانه‌های دیجیتالی تأثیر مثبت و معنادار دارد. این یافته با نتایج پژوهش‌های (آرام، ۱۳۸۸)، (زنده‌دل‌نوبری، ۱۳۸۹)، (ملک‌الکلامی، ۱۳۹۰)، (نورایی، ۱۳۹۱)، ارنست چانگ و هو ( Ernest Chang & Ho, 2006) ، کوزما (Kuzma, 2010) و تینتاماسیک (Tintamusik, 2013) همخوانی دارد. مطابق با این یافته، مطابق با این یافته، توسعهٔ سیستم های اطلاعاتی در کتابخانه‌ها و امنیت منابع انسانی نقش زیادی در حفظ امنیت اطلاعات ایفا می‌کنند. کتابخانه‌هایی که توانایی فراهم‌آوری و توسعهٔ سیستم‌های اطلاعاتی را دارند، به امنیت اطلاعات دست خواهند یافت. بنابراین هم مدیران و هم متصدیان امر دربارهٔ توسعهٔ سیستم‌های اطلاعاتی و ایجاد امنیت منابع انسانی اهمیت قائل شوند. همچنین نتایج نشان داد، حفاظت اطلاعات بر امنیت اطلاعات کتابخانه‌های دیجیتالی تأثیر مثبت و معنادار دارد. این یافته با نتایج پژوهش‌های (آرام، ۱۳۸۸)، (زنده‌دل نوبری ۱۳۸۹)، (ملک‌الکلامی، ۱۳۹۰)، (نورایی، ۱۳۹۱)، ارنست چانگ و هو (Ernest Chang & Ho, 2006)، کوزما (Kuzma, 2010 ) و تینتاماسیک (۲۰۱۳) همخوانی دارد. این یافته نشان می‌دهد، نحوهٔ استفاده و کنترل دستیابی به منابعی که به اشتراک گذاشته شده‌اند، از مهمترین هدف‌های یک سیستم امنیتی در شبکه است. هر سازمان برای حفاظت از اطلاعات ارزشمند، باید به راهبرد خاصی پایبند باشد و براساس آن سیستم امنیتی را پیاده‌سازی و اجرا نماید. بی‌تردید، امنیت بلندمدت منابع دیجیتالی و ارتقای دسترس‌پذیر میراث مکتوب که هدف‌های اساسی کتابخانه‌های دیجیتالی است، بدون لحاظ‌کردن مسائل حفاظتی امکان تحقق نخواهد یافت.

در مجموع، نتایج، اثر متغیرهای خط‌مشی امنیت اطلاعات، معماری اطلاعات، سازمان‌دهی امنیت اطلاعات، توسعهٔ سیستم‌های اطلاعاتی، امنیت منابع انسانی و حفاظت محتوا بر امنیت اطلاعات در کتابخانه‌های دیجیتالی را تأیید می‌کند. یافته‌های به‌دست‌آمده بر اهمیت این متغیرها برای کتابخانه‌های دیجیتالی به‌منظور تأثیرگذاری بر مدیریت امنیت اطلاعات تأکید می‌کند. در این پژوهش، فقط کتابخانه‌های دیجیتالی دانشگاه‌های تهران بررسی شد؛ بنابراین تعمیم یافته‌های این پژوهش به دیگر قلمروها با محدودیت مواجه است. همچنین یافته‌ها براساس داده‌های خود گزارش‌دهی هستند. پیشنهاد می‌شود، در پژوهش‌های آینده از روش‌های تحقیق کیفی و آمیخته برای فهم عمیق‌تر عوامل مؤثر بر امنیت اطلاعات کتابخانه‌های دیجیتالی استفاده شود.

سیستم‌ها و معماری‌های سازمانی و ممیزی کمک شایانی به استقرار سیستم‌های امنیت در سازمان‌ها (باتوجه‌به ضرورت این استقرار و زمان‌بر بودن آن) خواهند نمود. پایه‌ریزی تحقیقات دربارهٔ استقرار سیستم‌های سازمانی و معماری‌های مختلف، یکی از نیازمندی‌های ضروری محسوب می‌شود و لازم است تا محققان قدم‌های اساسی در این جهت بردارند. پیاده‌سازی سیستم‌های بهینهٔ تعریف‌شده، نیاز اعتمادسازی در سازمان‌ها و ارائهٔ منابع تحقیقات به سازمان‌ها در پذیرش این معماری‌ها تاثیرگذار خواهند بود.د. همچنین نرم‌افزاری و اتوماتیک‌کردن سیستم مدیریت امنیت و رعایت ملزومات از طرف کارمندان و ممیزی از طرف کارمندان و ممیزان به‌کمک سیستم‌های کاراتر می‌تواند به بلوغ سازمان و بالابردن امنیت کمک نماید. در پایان، برای بهبود در برقراری امنیت در سیستم‌های اطلاعاتی سرویس‌گرا، راهکارهایی ارائه شده است که این راهکارها را می‌توان به دو دستهٔ کلی تقسیم کرد. دستهٔ اول، راهکارهایی است که مشابه راهکارهای امنیتی در سایر سیستم‌های اطلاعاتی است مانند استفاده از اصول رمزنگاری در قسمت احراز هویت یا تکثیر سرویس‌ها برای افزایش سطح دسترسی. دستهٔ دوم، راهکارهای هستند که بیشتر به معماری سرویس‌گرا اختصاص دارند مانند استفاده از گذرگاه سرویس سازمانی برای اجرای کنترل‌های امنیتی در قسمت طراحی معماری، استفاده از WS-security برای امنیت سطح پیام و... . انتظار می‌رود، ابعاد امنیتی و راهکارهای ارائه‌شده، تا اندازه‌ای به تصمیم‌گیری بهتر مدیران و مجریانی کمک کند که مسئول برقراری سیستم‌های مدیریت امنیت در سیستم‌های اطلاعات سازمانی با معماری سرویس‌گرا هستند. همچنین سیستم بهینهٔ مدیریت امنیت را در سیستم‌های اطلاعاتی سازمانی توسعه‌یافته با معماری سرویس‌گرا تا حدزیادی برقرار کند.

## فهرست منابع

آرام، محمدرضا. (۱۳۸۸). بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی (پایان‌نامهٔ کارشناسی ارشد). دانشگاه شهید بهشتی، تهران.

باغبان‌زاده، محبوبه. (۱۳۹۳). شناسایی و اولویت‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی ANP و DEMATEL فازی (پایان نامه کارشناسی ارشد) . دانشگاه علم و هنر، .یزد.

زنده‌دل‌نوبری، بابک. (۱۳۸۹). ارائه مدلی جهت رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها (پایان‌نامه کارشناسی ارشد).دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران.

سادوسکای، جورج. (۱۳۸۴). راهنمای امنیت فناوری اطلاعات (مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی، مترجمان). تهران: دبیرخانه شورای عالی اطلاع‌رسانی.

ملک‌الکلامی، میلا. (۱۳۹۰). ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران براساس استاندارد بین‌المللی ایزو/ آی.ای.سی.۲۷۰۰۲، (پایان نامه کارشناسی ارشد). دانشگاه علامه طباطبایی، تهران.

ملک‌الکلامی، میلا. (۱۳۹۲)، ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد بین المللی ایزو/ آی.ای.سی. *پردازش و مدیریت اطلاعات*، ۲۸ (۴)، ۹۱۶-۸۹۵

مؤسسه استاندارد و تحقیقات صنعتی ایران. (۱۳۸۷). فن‌آوری اطلاعات‌فنون امنیتی‌آیین کار مدیریت امنیت اطلاعات، استاندارد ایزو/ آی.ای.سی ۲۷۰۰۲. بازیابی شده در ۱۱اردیبهشت‌ماه۱۳۹۵ http://www.isiri.org/portal/files/std/27002.pdf

میردامادی، مهدی. (۱۳۸۷). ضرورت توجه‌به امنیت اطلاعات: پیش درآمدی بر مباحث امنیت. ماهنامه تحلیلگران عصر اطلاعات (۱۹).

نورایی، فرزاد. (۱۳۹۱). بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعات ISMS در ایران (مطالعه موردی بانک دی)، (پایان نامه کارشناسی ارشد). دانشگاه سیستان و بلوچستان، زاهدان.

Briney, A. (2001). 2001 industry survey. *Information security*, 34-47. lfca.net/Reference%20Documents/2001%20Information%20Security%20Survey.pdf 5/2/2017

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361. Retrieved from https://www.emeraldinsight.com/doi/10.1108/02635570610

Gonzalez, J. J., & Sawicka, A. (2002). A framework for hum 653498an factors in information security. *In Wseas international conference on information security, Rio de Janeiro* (pp. 448-187). Retrieved from www.wseas.us/e-library/conferences/brazil2002/papers/448-187.pdf . 9/8/2016

Honan, B., (2006). IT security-oommoditized, badly. *lnfosecurity Today*, 3(5), 5-41. doi: 10.1016/S1742-6847(06)70461-x

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities, Library Hi Tech, 28(3), 402–413. doi:10.1108/07378831011076657

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134.Retrieved From https://doi.org/10.1016/j.im.2014.10.009

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for effective information security management*. CRC Press.

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies*, *38(*1-2), 4-37. doi:10.1080/01402390.2014.977382

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Tintamusik, Y. (2010). Examining the relationship between organization systems and information security awareness, (Doctoral Dissertation). Business Administration. Northcentral University. Retrieved from https://eric.ed.gov/?id=ED516884

United States. White House Office. (2017, July 28). International strategy for cyberspace, prosperity, security, and openness in a networked world. Retrieved from https://www.hsdl.org/?view & did =5665